Prime polynomials in short intervals and in arithmetic progressions

Efrat Bank * Lior Bary-Soroker † Lior Rosenzweig ‡

March 13, 2013

In this paper we establish function field versions of two classical conjectures on prime numbers. The first says that the number of primes in intervals $(x, x+x^\epsilon]$ is about $x^\epsilon/\log x$ and the second says that the number of primes $p < x$, $p \equiv a \pmod d$, for $d^{1+\delta} < x$, is about $\frac{\pi(x)}{\phi(d)}$.

More precisely, we prove: Let $1 \le m < k$ be integers, let q be a prime power, and let f be a monic polynomial of degree k with coefficients in $\mathbb{F}_q$. Then there is a constant $c(k)$ such that the number N of prime polynomials $g = f + h$ with $\deg h \le m$ satisfies $|N - q^{m+1}/k| \le c(k)q^{m+\frac{1}{2}}$. Here we assume $m \ge 2$ if $\gcd(q, k(k-1)) > 1$ and $m \ge 3$ if q is even and $\deg f' \le 1$. We show that this estimation fails in the neglected cases.

Let $\pi_q(k)$ be the number of monic prime polynomials of degree k with coefficients in $\mathbb{F}_q$. For relatively prime $f, D \in \mathbb{F}_q[t]$ we prove that the number N' of monic prime polynomials $g \equiv f \pmod D$ of degree k satisfies $|N' - \frac{\pi_q(k)}{\phi(D)}| \le c(k)\frac{\pi_q(k)q^{-1/2}}{\phi(D)}$, as long as $1 \le \deg D \le k-3$ (or $\le k-4$ if $p = 2$ and $(f/D)'$ is constant).

We also generalize these results to other factorization types.

1. Introduction

We study two function field analogues of two classical problems in number theory concerning the number of primes in short intervals and in arithmetic progressions. We first introduce the classical problems and then formulate the results in function fields.

*School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel, efratban@post.tau.ac.il

†School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel, barylior@post.tau.ac.il

‡Department of Mathematics, KTH, SE-10044, Stockholm, Sweden, lior.rosenzweig@gmail.com

1.1. Primes in short intervals

Let $\pi(x) = \#\{0 < p \leq x \mid p \text{ is a prime}\}$ be the prime counting function. By the Prime Number Theorem (PNT)

$$\pi(x) \sim \frac{x}{\log x}, \quad x \to \infty.$$

Therefore one may expect that an interval $I = (x, x + \Phi(x)]$ of size $\Phi(x)$ starting at a large x contains about $\Phi(x)/\log x$ primes, i.e.

$$\pi(I) := \pi(x + \Phi(x)) - \pi(x) \sim \frac{\Phi(x)}{\log x}. \tag{1}$$

From PNT (1) holds for $\Phi(x) \sim cx$, for any fixed $0 < c < 1$. By Riemann Hypothesis (1) holds for $\Phi(x) \sim \sqrt{x}\log x$ or even $\Phi(x) \sim \epsilon\sqrt{x \log x}$ assuming a strong form of Montgomery's pair correlation conjecture [7]. Concerning smaller powers of x Granville conjectures [4, p. 7] that

Conjecture 1.1. *If $\Phi(x) > x^\epsilon$ then (1) holds.*

But even for $\Phi(x) = \sqrt{x}$ Granville says [5, p. 73]:

> *we know of no approach to prove that there are primes in all intervals $[x, x + \sqrt{x}]$.*

Heath-Brown [6], improving Huxley [8], proves Conjecture 1.1, unconditionally, for $x^{\frac{7}{12}-\epsilon(x)} \leq \Phi(x) \leq \frac{x}{\log^4 x}$, where $\epsilon(x) \to 0$.

We note that for extremely short intervals (e.g. for $\Phi(x) = \log x \frac{\log\log x \log\log\log\log x}{\log\log\log x}$) (1) fails [12] uniformly, but may hold for almost all x, see [13] and the survey [5, Section 4].

1.2. Primes in arithmetic progressions

Let $\pi(x; d, a)$ denote the number of primes $p \leq x$ such that $p \equiv a \pmod{d}$. Then the Prime Number Theorem for arithmetic progressions says that if a and d are relatively prime and fixed, then

$$\pi(x; d, a) \sim \frac{\pi(x)}{\phi(d)}, \quad x \to \infty, \tag{2}$$

where $\pi(x)$ is the prime counting function and $\phi(d)$ is the Euler totient function, giving the number of positive integers i up to d with $\gcd(i, d) = 1$.

In many applications it is crucial to allow the modulus d to grow with x. The interesting range is $d < x$ since if $d \geq x$, there can be at most one prime in the arithmetic progression $p \equiv i \pmod{d}$. A classical conjecture is the following (in a slightly different form see [11, Conjecture 13.9]).

Conjecture 1.2. *For every $\delta > 0$, (2) holds in the range $d^{1+\delta} < x$.*

Concerning results on this conjecture Granville says [5, p. 69]:

> *... the best proven results have x bigger than the exponential of a power of q* (Granville's q is our d) *far larger than what we expect. If we are prepared to assume the unproven Generalized Riemann Hypothesis we do much better, being able to prove that the primes up to $q^{2+\delta}$ are equally distributed amongst the arithmetic progressions* $\bmod q$*, for q sufficiently large, though notice that this is still somewhat larger than what we expect to be true.*

In this work we establish function field analogues of Conjectures 1.1 and 1.2 for certain intervals of parameters ϵ, δ which may be arbitrary small, and in particular breaking the barriers $\epsilon = 1/2$ in the former and $\delta = 1$ in the latter. This indicates that Conjectures 1.1 and 1.2 should hold. A crucial ingredient is a type of Hilbert's irreducibility theorem over finite fields [2].

2. Results in function fields

Let $\mathcal{P}_{\leq k}$ be the space of polynomials of degree at most k over $\mathbb{F}_q$ and $\mathcal{M}(k,q) \subseteq \mathcal{P}_{\leq k}$ the subset of monic polynomials of degree k. If $\deg f = k$, we let $\|f\| = q^k$.

2.1. Short intervals

Let $\pi_q(k) = \#\{g \in M(k,q) \mid g \text{ is a prime polynomial}\}$ be the prime polynomial counting function. The Prime Polynomial Theorem (PPT) asserts that

$$\pi_q(k) = \frac{q^k}{k} + O\left(\frac{q^{k/2}}{k}\right).$$

An interval I around $f \in \mathcal{M}(k,q)$ is defined as

$$I = I(f,m) = \{g \in \mathbb{F}_q[t] \mid \|f - g\| \leq q^m\} = f + \mathcal{P}_{\leq \lfloor m \rfloor}.$$

If $m \geq k$, then $I(f,m) = \mathcal{P}_{\leq m}$, and so the PPT gives the number of primes there. The interesting intervals are the *short intervals*, i.e. when $m < k$. In particular $\mathcal{M}(k,q) = I(t^k, k-1)$. We note that all the polynomials in a short interval around a monic polynomial are monic.

For a short interval I let $\pi_q(I) = \#\{g \in I \mid g \text{ is a prime polynomial}\}$. The expected analogy to (1) is

$$\pi_q(I(f,m)) \sim \frac{|I(f,m)|}{k} = \frac{q^{\lfloor m \rfloor + 1}}{k}, \tag{3}$$

for $f \in \mathcal{M}(k,q)$ and $0 < m < k$.

Keating and Rudnick [9] study the variance of primes in short intervals in the limit $q \to \infty$. From their result it follows in a standard way that (3) holds almost everywhere for $m \leq k - 3$, see Appendix A for details.

We show that (3) holds everywhere:

Theorem 2.1. *Let k be a positive integer. Then there exists a constant $c(k) > 0$ depending only on k such that for any*

- *prime power $q = p^\nu$,*
- *integer $1 \le m < k$, and*
- *a short interval $I = I(f, m)$ around $f \in \mathcal{M}(k, q)$*

we have

$$\left| \pi_q(I) - \frac{q^{m+1}}{k} \right| \le c(k) q^{m+\frac{1}{2}},$$

provided $2 \le m$ if $p \mid k(k-1)$ and provided $3 \le m$ if $p = 2$ and $\deg f' \le 1$.

To compare with Conjecture 1.1 we note that x corresponds to q^k, hence an interval of length x^ϵ corresponds to $I(f, \epsilon k)$, $f \in \mathcal{M}(k, q)$. Thus for any fixed k, for every $\frac{3}{k} \le \epsilon \le 1$, and for every sequence of intervals $I_q = I_q(f_q, \epsilon k)$,

$$\pi_q(I_q) \sim \frac{|I_q|}{k}, \quad q \to \infty.$$

(In fact it is possible to consider $\epsilon \ge \frac{1}{k}$ for those intervals I_q, $q = p^\nu$, for which $p \nmid k(k-1)$ and $\epsilon \ge \frac{2}{k}$ if $p \ne 2$ or $p = 2$ and $\deg f_q' \ge 2$.) The conclusion is that a precise analogue of Conjecture 1.1 for $\frac{3}{k} \le \epsilon \le 1$ holds. In particular we go below the barrier $\epsilon = \frac{1}{2}$, and by enlarging k, ϵ can be made arbitrary small.

In Section 6 we discuss the cases which are not included in Theorem 2.1 by studying the intervals $I(t^k, m)$. In particular we show that (3) fails if $m = 0$, or if $m = 1$ and $p \mid k(k-1)$. We do not know whether (3) holds true in the remaining case $p = m = 2$ and $\deg f' \le 1$.

2.2. Primes in arithmetic progressions

For relatively prime $f, D \in \mathbb{F}_q[t]$ let

$$\pi_q(k; D, f) = \#\{h = f + Dg \in \mathcal{M}(k, q) \mid h \text{ is a prime polynomial}\}.$$

The Prime Polynomial Theorem for arithmetic progressions says that

$$\pi_q(k; D, f) = \frac{\pi_q(k)}{\phi(D)} + O\left(\frac{q^{k/2}}{k} \deg D \right). \tag{4}$$

Here $\phi(g)$ is the function field Euler totient function, giving the number of units in $\mathbb{F}_q[t]/g\mathbb{F}_q[t]$.

In analogy to the classical case we want to allow $\deg D$ to grow with k. The interesting range of parameters is $\deg D > k$, because if $\deg D \ge k$, there is at most one monic prime in the arithmetic progression $h \equiv f \mod D$ of degree k.

We note that

$$\phi(D) \sim q^{\deg D}, \quad q \to \infty.$$

Therefore, if $2 \deg D < k - \delta$, then (4) gives that

$$\pi_q(k; D, f) \sim \frac{\pi_q(k)}{\phi(D)}, \quad q \to \infty.$$

On the other hand (4) gives nothing when $2 \deg D \geq k$.

In analogy with (2) one may expect that

$$\pi_q(k; D, f) \sim \frac{\pi_q(k)}{\phi(D)} \tag{5}$$

as long as $(1 + \delta) \deg D \leq k$.

Keating and Rudnick [9] calculate the variance of the number of primes in arithmetic progressions in function fields. From their work (5) holds true almost everywhere, in a standard way.

We show (5) everywhere:

Theorem 2.2. *Let k be a positive integer. Then there exists a constant $c(k) > 0$ depending only on k such that for any*

- *prime power $q = p^\nu$,*
- *$2 \leq m < k$*
- *monic modulus $D \in \mathbb{F}_q[t]$ with $\deg D = k - m - 1$,*
- *and $f \in \mathbb{F}_q[t]$,*

we have

$$\left| \pi_q(k; D, f) - \frac{\pi_q(k)}{\phi(D)} \right| \leq c(k) q^{m + \frac{1}{2}},$$

provided $(f/D)'$ is not constant if $p = m = 2$. (Note that $\frac{\pi_q(k)}{\phi(D)} \sim \frac{q^{k - \deg D}}{k} = \frac{q^{m+1}}{k}$ as $q \to \infty$.)

To compare with Conjecture 1.2 we note that x corresponds to q^k, d corresponds to $q^{\deg D}$ and the condition $d^{(1+\delta)} < x$ translates to $(1 + \delta) \deg D < k$. Thus for any fixed k and $\frac{4}{k-4} \leq \delta$ and for any sequence of $(D_q, f_q)_q$ with $D_q, f_q \in \mathbb{F}_q[t]$ such that D is monic and $(1 + \delta) \deg D_q < k$ we have

$$\pi_q(k; D_q, f_q) \sim \frac{\pi_q(k)}{\phi(D_q)}, \quad q \to \infty.$$

(In fact we may take $\frac{3}{k-3} \leq \delta$ if q is odd or if $(f_q/D_q)'$ is not constant.) The conclusion is that a perfect analogue of Conjecture 1.2 for $\frac{4}{k-4} \leq \delta$ holds. In particular we go below the barrier $\delta = 1$ and by enlarging k, δ can be made arbitrary small. This indicates that Conjecture 1.2 should hold for any $\delta > 0$.

2.3. Other factorization types

Our method allows us to count polynomials with any given factorization type. Let us start by setting up the notation.

The degrees of the primes in the factorization of a polynomial $f \in \mathbb{F}_q[t]$ to a product of prime polynomials gives a partition of $\deg f$, denoted by λ_f. Similarly the lengths of the cycles in the factorization of a permutation $\sigma \in S_k$ to a product of disjoint cycles induce a partition, λ_σ, of k. For a partition λ of k we denote the probability for $\sigma \in S_k$ to have $\lambda_\sigma = \lambda$ by

$$P(\lambda) = \frac{\#\{\sigma \in S_k \mid \lambda_\sigma = \lambda\}}{k!}. \tag{6}$$

We note that if λ is the partition to one part, then $\lambda_f = \lambda$ if and only if f is prime and $P(\lambda) = \frac{(k-1)!}{k!} = \frac{1}{k}$.

Let k be a positive integer and λ a partition of k. For a short interval $I = I(f, m)$ with $f \in \mathcal{M}(k, q)$ we define the counting function

$$\pi_q(I; \lambda) = \#\{g \in I \mid \lambda_g = \lambda\}.$$

We generalize Theorem 2.1:

Theorem 2.3. *Let k be a positive integer. Then there exists a constant $c(k) > 0$ depending only on k such that for any*

- *partition λ of k,*
- *prime power $q = p^\nu$,*
- *integer $1 \le m < k$, and*
- *a short interval $I = I(f, m)$ around $f \in \mathcal{M}(k, q)$*

we have

$$\left|\pi_q(I; \lambda) - P(\lambda) q^{m+1}\right| \le c(k) q^{m+\frac{1}{2}},$$

provided $2 \le m$ if $p \mid k(k-1)$ and provided $3 \le m$ if $p = 2$ and $\deg f' \le 1$.

For relatively prime $f, D \in \mathbb{F}_q[t]$ with D monic we define the counting function

$$\pi_q(k; D, f; \lambda) = \#\{g \equiv f \pmod{D} \mid \deg g = k \text{ and } \lambda_g = \lambda\}.$$

We generalize Theorem 2.2:

Theorem 2.4. *Let k be a positive integer. Then there exists a constant $c(k) > 0$ depending only on k such that for any*

- *partition λ of k,*
- *prime power $q = p^\nu$,*

- $2 \le m < k$
- *monic modulus* $D \in \mathbb{F}_q[t]$ *with* $\deg D = k - m - 1$, *and*
- $f \in \mathbb{F}_q[t]$,

we have

$$\left| \pi_q(k; D, f; \lambda) - \frac{\pi_q(k; \lambda)}{\phi(D)} \right| \le c(k) q^{m+\frac{1}{2}},$$

provided $(f/D)'$ *is not constant if* $p = m = 2$. *(Note that* $\frac{\pi_q(k;\lambda)}{\phi(D)} \sim P(\lambda) q^{k-\deg D} = P(\lambda) q^{m+1}$ *as* $q \to \infty$. *)*

3. Auxiliary results

3.1. Specializations

We briefly recall some definitions and basic facts on specializations, see [2, Section 2.1] for more details and proofs. Let

K be a field with algebraic closure $\tilde{K}$,
$\mathrm{Gal}(K) = \mathrm{Aut}(\tilde{K}/K)$ the absolute Galois group of K,
$W = \operatorname{Spec} S$ and $V = \operatorname{Spec} R$ absolutely irreducible smooth affine K-varieties,
$\rho\colon W \to V$ a finite separable morphism which is generically Galois,
F/E the function field Galois extension that corresponds to ρ,
K-rational point $\mathfrak{p} \in V(K)$ that is étale in W, and
$\mathfrak{P} \in \rho^{-1}(\mathfrak{p})$.

Then $\mathfrak{p}$ induces a homomorphism $\phi_{\mathfrak{p}}\colon R \to K$ that extends to a homomorphism $\phi_{\mathfrak{P}}\colon S \to \tilde{K}$ (via the inclusion $R \to S$ induced by ρ). Since $\mathfrak{p}$ is étale in W, we have a homomorphism $\mathfrak{P}^*\colon \mathrm{Gal}(K) \to \mathrm{Gal}(F/E)$ such that

$$\phi_{\mathfrak{P}}(\mathfrak{P}^*(\sigma)(x)) = \sigma(\phi_{\mathfrak{P}}(x)), \quad \forall x \in S,\ \forall \sigma \in \mathrm{Gal}(K). \tag{7}$$

For every other $\mathfrak{Q} \in \rho^{-1}(\mathfrak{p})$ there is $\tau \in \mathrm{Gal}(F/E)$ such that $\phi_{\mathfrak{Q}} = \phi_{\mathfrak{P}} \circ \tau$. Thus, by (7), $\mathfrak{Q}^* = \tau^{-1}\mathfrak{P}^*\tau$ and vice-versa every $\tau^{-1}\mathfrak{P}^*\tau$ comes from a point $\mathfrak{Q} \in \rho^{-1}(\mathfrak{p})$. Hence $\mathfrak{p}^* = \{\mathfrak{Q}^* \mid \mathfrak{Q} \in \rho^{-1}(\mathfrak{p})\}$ is the orbit of $\mathfrak{P}^*$ under the conjugation action of $\mathrm{Gal}(F/E)$.

The key ingredients in the proof of the following proposition are the Lang-Weil estimates [10, Theorem 1] and the field crossing argument (as utilized in [2, Proposition 2.2]).

Proposition 3.1. *Let* k, m, *and* B *be positive integers, let* λ *be a partition of* k, *let* $\mathbb{F}$ *be an algebraic closure of* $\mathbb{F}_q$, *and let* $\mathcal{F} \in \mathbb{F}_q[A_0, \dots, A_m, t]$ *be a polynomial that is separable in* t *with* $\deg \mathcal{F} \le B$ *and* $\deg_t \mathcal{F} = k$. *Assume that* $\mathcal{F}$ *is separable in* t *and*

$$\mathrm{Gal}(\mathcal{F}, \mathbb{F}(A_0, \dots, A_m)) = S_k.$$

Then there is a constant $c(m, B)$ that depends only on m and B such that if we denote by $N = N(\mathcal{F}, q)$ the number of $(a_0, \dots, a_m) \in \mathbb{F}_q^{m+1}$ such that $f = \mathcal{F}(a_0, \dots, a_m, t)$ has factorization type $\lambda_f = \lambda$, then

$$\left|N - P(\lambda)q^{m+1}\right| \leq c(m, B)q^{m+1/2},$$

where $P(\lambda)$ is defined in (6)*.*

Proof. Let $\mathbf{A} = (A_0, \dots, A_m)$ and F the splitting field of $\mathcal{F}$ over $\mathbb{F}_q(\mathbf{A})$. Since

$$S_k = \mathrm{Gal}(\mathcal{F}, \mathbb{F}(\mathbf{A})) = \mathrm{Gal}(F \cdot \mathbb{F}/\mathbb{F}(\mathbf{A})) \leq \mathrm{Gal}(F/\mathbb{F}_q(\mathbf{A})) \leq S_k,$$

all inequalities are in fact equalities and $\mathbb{F}_q = F \cap \mathbb{F}$. In particular, $\alpha\colon \mathrm{Gal}(F/\mathbb{F}_q(\mathbf{A})) \to \mathrm{Gal}(F \cap \mathbb{F}/\mathbb{F}_q) = 1$, so

$$\ker \alpha = S_k. \tag{8}$$

Since $\mathrm{Gal}(\mathbb{F}_q) = \langle\varphi\rangle \cong \hat{\mathbb{Z}}$ with φ being the Frobenius map $x \mapsto x^q$, the homomorphisms $\theta\colon \mathrm{Gal}(\mathbb{F}_q) \to S_k$ can be parametrized by permutations $\sigma \in S_k$. Explicitly, each $\sigma \in S_k$ gives rise to $\theta_\sigma\colon \mathrm{Gal}(\mathbb{F}_q) \to S_k$ defined by $\theta_\sigma(\varphi) = \sigma$. Let $\mathcal{C}$ be the conjugacy class of all permutations σ with $\lambda_\sigma = \lambda$ and let $\Theta = \{\theta_\sigma \mid \sigma \in \mathcal{C}\}$. Fix $\theta \in \Theta$. Clearly $\#\Theta = \#\mathcal{C}$, so by (8) we have

$$\frac{\#\ker\alpha}{\#\Theta} = \frac{\#S_k}{\#C} = \frac{1}{P(\lambda)}. \tag{9}$$

Let Z be the closed subset of $\mathbb{A}^{m+1} = \operatorname{Spec}\mathbb{F}_q[\mathbf{A}]$ defined by $D = \mathrm{disc}_t(\mathcal{F}) = 0$ and $V = \mathbb{A}^{m+1} \smallsetminus Z = \operatorname{Spec}\mathbb{F}_q[\mathbf{A}, D^{-1}]$. By assumption $\mathcal{F}$ is separable in t, so D is a nonzero polynomial of degree depending only on B. By [10, Lemma 1], there exists a constant $c_1 = c_1(m, B)$ such that

$$\#Z(K) \leq c_1 q^m. \tag{10}$$

Let $u_1, \dots, u_k$ be the roots of $\mathcal{F}$ in some algebraic closure of $\mathbb{F}(A_0, \dots, A_m)$ and let $W = \operatorname{Spec}\mathbb{F}_q[u_1, \dots, u_k, D^{-1}] \subseteq \mathbb{A}^{k+1}$. Then W is an irreducible smooth affine $\mathbb{F}_q$-variety of degree bounded in terms of $B = \deg\mathcal{F}$ and the embedding $\mathbb{F}_q[\mathbf{A}, D^{-1}] \to \mathbb{F}_q[u_1, \dots, u_k, D^{-1}]$ induces a finite separable étale morphism $\rho\colon W \to V$.

We apply [2, Proposition 2.2] to get an absolutely irreducible smooth $\mathbb{F}_q$-variety $\widehat{W}$ together with a finite separable étale morphism $\pi\colon \widehat{W} \to V$ with the following properties:

i. Let $U \subseteq V(\mathbb{F}_q)$ be the set of $\mathfrak{p} \in V(\mathbb{F}_q)$ that are étale in W and such that $\mathfrak{p}^* = \Theta$. Then $\pi(\widehat{W}(\mathbb{F}_q)) = U$.

ii. For every $\mathfrak{p} \in U$,

$$\#(\pi^{-1}(\mathfrak{p}) \cap \widehat{W}(\mathbb{F}_q)) = \frac{\#\ker\alpha}{\#\Theta} = \frac{1}{P(\lambda)}.$$

(See (9) for the last equality.)

By the construction of $\widehat{W}$ in *loc. cit.* it holds that $\widehat{W}_L = W_L$, for some finite extension $L/\mathbb{F}_q$ (where subscript L indicates the extension of scalars to L). Hence $\widehat{W}$ and W have the same degree, which is bounded in terms of B. Thus, by [10, Theorem 1], there is a constant $c_2 = c_2(m, B)$ such that

$$|\#\widehat{W}(\mathbb{F}_q) - q^{m+1}| \leq c_2 q^{m+1/2}. \tag{11}$$

Applying (ii) gives $P(\lambda) \cdot \#\pi(\widehat{W}(\mathbb{F}_q)) = \#\widehat{W}(\mathbb{F}_q)$. So multiplying (11) by $P(\lambda)$ implies

$$|\#\pi(\widehat{W}(\mathbb{F}_q)) - P(\lambda)q^{m+1}| \leq P(\lambda)c_2 q^{m+1/2} \leq c_2 q^{m+1/2}. \tag{12}$$

Since for $\mathfrak{p} = (a_0, \ldots, a_m) \in V(\mathbb{F}_q) \subseteq \mathbb{F}_q^{m+1}$ we have $\mathfrak{p}^* = \Theta$ if and only if the orbit type of $\mathfrak{p}^*$ is λ (in the sense of [2, p. 859]). Thus $\lambda_{\mathcal{F}(a_0,\ldots,a_m,t)} = \lambda$ if and only $\mathfrak{p}^* = \Theta$ ([2, Lemma 2.1]). Let

$$X = \{\mathfrak{p} = (a_0, \ldots, a_m) \in \mathbb{F}_q^{m+1} \mid \lambda_{\mathcal{F}(a_0,\ldots,a_m,t)} = \lambda \text{ and } D(a_0, \ldots, a_m) \neq 0\}.$$

Then $N = \#X$. Equation (i) gives $X \cap V(\mathbb{F}_q) = \pi(\widehat{W}(\mathbb{F}_q))$. Since $V = \mathbb{A}^{m+1} \smallsetminus Z$, it follows from (10) and (12) that

$$\begin{aligned}
\left|N - P(\lambda)q^{m+1}\right| &= \left|\#X - P(\lambda)q^{m+1}\right| \\
&= \left|\#(X \cap V(\mathbb{F}_q)) + \#(X \cap Z(\mathbb{F}_q)) - P(\lambda)q^{m+1}\right| \\
&\leq \left|\#(X \cap V(\mathbb{F}_q)) - P(\lambda)q^{m+1}\right| + \#(X \cap Z(\mathbb{F}_q)) \\
&\leq \left|\pi(\widehat{W}(\mathbb{F}_q)) - P(\lambda)q^{m+1}\right| + \#Z(\mathbb{F}_q) \\
&\leq c_2 q^{m+1/2} + c_1 q^m \leq c(m, B)q^{m+1/2},
\end{aligned}$$

where $c = c_1 + c_2$. □

3.2. Calculating a Galois Group

Lemma 3.2. *Let F be an algebraically closed field, $\mathbf{A} = (A_0, \ldots, A_m)$ an m-tuple of variables with $m \geq 1$, and $f, g \in K[t]$ relatively prime polynomials. Then $\mathcal{F}(\mathbf{A}, t) = f + g(\sum_{i=1}^m A_i t^i)$ is separable in t and irreducible in the ring $F(\mathbf{A})[t]$.*

Proof. Since $\mathcal{F}$ is linear in A_0 and since f, g are relatively prime, it follows that $\mathcal{F}$ is irreducible in $F[\mathbf{A}, t]$, hence by Gauss' lemma also in $F(A)[t]$. Take $\alpha \in F$ with $g(\alpha) \neq 0$. Then

$$\mathcal{F}'(\alpha) = f'(\alpha) + g'(\alpha)A_0 + g(\alpha)A_1 \neq 0,$$

hence $\mathcal{F}' \neq 0$, so $\mathcal{F}$ is separable. □

Lemma 3.3. *Let F be an algebraically closed field, $\mathbf{A} = (A_0, \ldots, A_m)$ an m-tuple of variables with $m \geq 2$, and $f, g \in K[t]$ relatively prime polynomials with $\deg f > \deg g$. The Galois group G of $\mathcal{F}(\mathbf{A}, t) = f + g(\sum_{i=1}^m A_i t^i)$ over $F(\mathbf{A})$ is doubly transitive (with respect to the action on the roots of $\mathcal{F}$).*

Proof. By replacing t by $t+\alpha$, where $\alpha \in F$ is a root of f, we may assume that $f(0) = 0$, hence $f_0(t) = f(t)/t$ is a polynomial. By Lemma 3.2 the group G is transitive. The image of $\mathcal{F}$ under the substitution $A_0 = 0$ is

$$\bar{\mathcal{F}} = f + g\big(\sum_{i=1}^{m} A_i t^i\big) = t\big(f_0 + g\big(\sum_{i=0}^{m-1} A_i t^{i-1}\big)\big).$$

Lemma 3.2 then gives that $f_0 + g\big(\sum_{i=0}^{m-1} A_i t^{i-1}\big)$ is separable and irreducible. Hence the stabilizer of the root $t = 0$ in the Galois group of $\bar{\mathcal{F}}$ acts transitively on the other roots. But since $\bar{\mathcal{F}}$ is separable, its Galois group embeds into G, so the stabilizer of a root of $\mathcal{F}$ in G is transitive. Thus G is doubly transitive. □

For a rational function $\psi(t) \in F(t)$ the first and second Hasse-Schmidt derivatives of ψ are denoted by ψ' and $\psi^{[2]}$, respectively, and defined by

$$\psi(t+u) \equiv \psi(t) + \psi'(t)u + \psi^{[2]}(t)u^2 \mod u^3.$$

A trivial observation is that ψ' is the usual derivative of ψ and, if the characteristic of $F \neq 2$, then $\psi^{[2]} = \frac{1}{2}\psi''$.

Lemma 3.4. *Let $\psi(t) \in F(t)$ be a rational function with $\psi^{[2]}$ nonzero and A_1 a variable. Then $\psi'(t) + A_1$ and $\psi^{[2]}(t)$ have no common zeros.*

Proof. This is obvious since the roots of $\psi' + A_1$ are transcendental over F, while those of $\psi^{[2]}$ are algebraic. □

Lemma 3.5. *Let F be an algebraically closed field of characteristic $p \geq 0$, $m \geq 2$, $\mathbf{A} = (A_1, \ldots, A_m)$, $f, g \in F[t]$ relatively prime polynomials and put $\psi = f/g$ and $\Psi = \psi + \sum_{i=1}^{m} A_i t^i$. Assume $\deg f > \deg g + m$. Further assume that ψ' is not a constant if $p = m = 2$. Then the system of equations*

$$\begin{aligned} \Psi'(\rho_1) &= 0 \\ \Psi'(\rho_2) &= 0 \\ \Psi(\rho_1) &= \Psi(\rho_2) \end{aligned} \tag{13}$$

has no solution with distinct ρ_1, ρ_2 in an algebraic closure Ω of $F(\mathbf{A})$.

Proof. For short we write $\rho = (\rho_1, \rho_2)$. Let

$$-\varphi(t) = \left(\psi + \sum_{i=3}^{m} A_i t^i\right)' = \psi' + \sum_{i=3}^{m} i A_i t^{i-1} = \frac{f'g - fg'}{g^2} + \sum_{i=3}^{m} i A_i t^{i-1}.$$

Then $\Psi'(t) = 2A_2 t + A_1 - \varphi(t)$. If $p = m = 2$, then $\varphi = -\psi'$ which is not constant by assumption.

Let

$$\begin{aligned} c(\rho) &= \psi(\rho_1) - \psi(\rho_2) + \sum_{i=3}^{m} (\rho_1^i - \rho_2^i) A_i \\ &= \Psi(\rho_1) - \Psi(\rho_2) - ((\rho_1^2 - \rho_2^2)A_2 + (\rho_1 - \rho_2)A_1). \end{aligned}$$

The system of equations (13) defines an algebraic set $T \subseteq \mathbb{A}^2 \times \mathbb{A}^m$ in the variables $\rho_1, \rho_2, A_1, \ldots, A_m$. Let $\alpha\colon T \to \mathbb{A}^2$ and $\beta\colon T \to \mathbb{A}^m$ the projection maps. The system of equations (13) takes the matrix form

$$M(\rho) \cdot \left(\begin{smallmatrix} A_2 \\ A_1 \end{smallmatrix}\right) = B(\rho) = \left(\begin{smallmatrix} \varphi(\rho_1) \\ \varphi(\rho_2) \\ c(\rho) \end{smallmatrix}\right), \tag{14}$$

where $M(\rho) = \begin{pmatrix} 2\rho_1 & 1 \\ 2\rho_2 & 1 \\ \rho_2^2-\rho_1^2 & \rho_2-\rho_1 \end{pmatrix}$. For every $\rho \in U = \{\rho \mid \rho_1 \neq \rho_2,\ \varphi(\rho_i) \neq \infty, i = 1, 2\}$, the rank of $M(\rho)$ is 2. Thus the dimension of the fiber $\alpha^{-1}(\rho)$, for any $\rho \in U$, is at most $m-2$. Moreover, for a given $\rho \in U$, (14) is solvable if and only if $\operatorname{rank}(M|B) = 2$ if and only if $d(\rho) = \det(M|B) = 0$, that is the solution space (restricting to $\rho \in U$) lies in $d(\rho) = 0$.

It suffices to prove that $d(\rho)$ is a nonzero rational function in the variables $\rho = (\rho_1, \rho_2)$. Indeed, this implies that $\dim(\alpha(T)) \leq \dim\{d(\rho) = 0\} = 1$, so $\dim T \leq 1 + m - 2 < m$. Thus $\beta(T)$ does not contain the generic point of $\mathbb{A}^m$ which is $\mathbf{A} = (A_0, \ldots, A_m)$ and hence (13) has no solution with $\rho \in \Omega^2$.

A straightforward calculation gives

$$d(\rho) = (\rho_1 - \rho_2)(2c(\rho) + (\rho_1 - \rho_2)(\varphi(\rho_1) + \varphi(\rho_2))).$$

If $m \geq 3$, then the coefficient of A_3 in $2c(\rho) + (\rho_1 - \rho_2)(\varphi(\rho_1) + \varphi(\rho_2))$ is

$$2(\rho_1^3 - \rho_2^3) + 3(\rho_1^2 - \rho_2^2),$$

which is nonzero in any characteristic and we are done.

To this end assume $m = 2$. If $p = 2$, then $2c(\rho) = 0$. Since φ is not constant in this case, we have $\varphi(\rho_1) + \varphi(\rho_2) \neq 0$ and we are done.

Finally assume $m = 2$ and $p \neq 2$. Then $c(\rho) = \psi(\rho_1) - \psi(\rho_2)$ and $\phi = -\psi'$. We may assume without loss of generality that $f(0) = 0$ (and hence $\psi(0) = 0$). Since $f(t)/t + g(t)(A_2 t + A_1)$ is separable (Lemma 3.2), we can replace A_1 and A_2 by $A_1 + \alpha_1$ and $A_2 + \alpha_2$, respectively, and f by $f(t) + g(t)(\alpha_2 t^2 + \alpha_1 t)$, for suitably chosen $\alpha_1, \alpha_2 \in F$, to assume that $f(t)/t$ is separable. Since $\deg f(t) > \deg + m \geq 2$, this implies that $f(t)$ has at least one simple root, say α. Then α is a simple root of $\psi = f/g$. So $\psi'(\alpha) \neq 0$. Let $\beta \neq \alpha$ be another root of f, hence of ψ.

If $\psi'(\beta) = 0$, then we have $c(\alpha, \beta) = \psi(\alpha) - \psi(\beta) = 0$, so

$$d(\alpha, \beta) = -(\alpha - \beta)^2 \psi'(\alpha) \neq 0$$

and we are done. If $\psi'(\beta) \neq 0$, then β is a simple root of ψ, hence of f. But $\deg f > 2$, so there must be another root γ of ψ. If $d = 0$, then we must have

$$\begin{aligned} \frac{d(\alpha, \beta)}{-(\alpha - \beta)^2} &= 0 = \psi'(\alpha) + \psi'(\beta) \\ \frac{d(\alpha, \gamma)}{-(\alpha - \gamma)^2} &= 0 = \psi'(\alpha) + \psi'(\gamma) \\ \frac{d(\gamma, \beta)}{-(\gamma - \beta)^2} &= 0 = \psi'(\gamma) + \psi'(\beta). \end{aligned}$$

So $2\psi'(\alpha) = 0$. This contradiction, implies that $d \neq 0$, as needed. □

Proposition 3.6. *Let F be a field of characteristic $p \geq 0$, let $1 \leq m < k$, let $\mathbf{A} = (A_0, \ldots, A_m)$ an $(m+1)$-tuple of variables, and let $f, g \in F[t]$ be relatively prime polynomials with $\deg g + m < k = \deg f$. Assume*

1. *$2 \leq m$ if $\deg g > 0$,*
2. *$2 \leq m$ if $p \mid k(k-1)$, and*
3. *$(f/g)'$ is not constant if $p = m = 2$.*

Then the Galois group of $\mathcal{F}(\mathbf{A}, t) = f(t) + g(t)(\sum_{i=0}^{m} A_i t^i)$ over $F(\mathbf{A})$ is

$$\mathrm{Gal}\,(\mathcal{F}, F(\mathbf{A})) = S_k.$$

Proof. Let $\tilde{F}$ be an algebraic closure of F. Since $\mathrm{Gal}(\mathcal{F}, \tilde{F}(\mathbf{A})) \leq \mathrm{Gal}(\mathcal{F}, F(\mathbf{A})) \leq S_k$, we may replace, without loss of generality, F by $\tilde{F}$ to assume that F is algebraically closed.

If $p \nmid k(k-1)$ and $\deg g = 0$, the result follows from [3, Theorem 1] (note that $F(A_0, \ldots, A_m) = F(A_2, \ldots, A_{m-1})(A_0, A_1)$, hence the result for $m = 1$ in *loc. cit.* extends to $m > 1$).

Assume that $2 \leq m$. Then $G = \mathrm{Gal}(\mathcal{F}, F(\mathbf{A})) \leq S_k$ is doubly transitive by Lemma 3.3.

Let Ω be an algebraic closure of $F(A_1, \ldots, A_m)$ and consider the map $\Psi\colon \mathbb{P}^1_\Omega \to \mathbb{P}^1_\Omega$ defined locally by $t \mapsto -A_0 := \frac{f(t)}{g(t)} + \sum_{i=1}^{m} A_i t^i$. The numerator of $\Psi' = \frac{f'g - g'f}{g^2} + \sum_{i=1}^{m} i A_i t^i$ is

$$f'g - g'f + g^2(\cdots + 2A_2 t + A_1).$$

If $m \geq 3$ or if $p \neq 2$, this numerator has positive degree. If $p = m = 2$, then this numerator is $f'g - g'f + g^2 A_1$, so it is not constant by (3). In any case, the numerator of Ψ', hence Ψ', has a root, say $\alpha \in \Omega$. Then Ψ is ramified at $t = \alpha$. Lemma 3.4 says that the orders of ramifications are ≤ 2, so the equation $\Psi(t) = \Psi(\alpha)$ has at most double roots in Ω. Lemma 3.5 says that the critical values are distinct, so $\Psi(t) = \Psi(\alpha)$ has at least $k-1$ solutions. But since α is a ramification point, the fiber over $\Psi(\alpha)$ is with exactly one double points. Hence the inertia group over $\Psi(\alpha)$ permutes two roots of

$$\mathcal{F}(\mathbf{A}, t) = g(t)(\Psi(t) + A_0),$$

and fixes the other roots (cf. [1, Proposition 2.6]). In other words G contains a transposition. Therefore $G = S_k$ [14, Lemma 4.4.3]. □

4. Proof of Theorems 2.1 and 2.3

Since Theorem 2.1 is a special case of Theorem 2.3 it suffices to prove the latter.

Let k be a positive integer, λ a partition of k, $q = p^\nu$ a prime power, $1 \leq m < k$, and $I = I(f, m)$ a short interval around $f \in \mathcal{M}(k, q)$. Assume $2 \leq m$ if $p \mid k(k-1)$ and assume $3 \leq m$ if $p = 2$ and $\deg f' \leq 1$. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$.

Let $\mathcal{F} = f + \sum_{i=0}^{m} A_i t^i$. Then $\mathcal{F}$ satisfies the assumptions of Proposition 3.6, so $\mathrm{Gal}(\mathcal{F}, \mathbb{F}(A_0, \ldots, A_m)) = S_k$.

Since $\deg \mathcal{F} = \deg_t \mathcal{F} = \deg f = k$ and $m < k$, by Proposition 3.1, the number N of $(a_0, \ldots, a_m) \in \mathbb{F}_q^{m+1}$ such that $f + \sum_{i=0}^{m} a_i t^i$ has factorization type λ satisfies

$$\left|N - P(\lambda) q^{m+1}\right| \leq c(k) q^{m+1/2},$$

where $c(k) > 0$ is a constant depending only on k (and not on f, q). This finishes the proof since by definition $N = \pi_q(I(f, m); \lambda)$. □

5. Proof of Theorems 2.2 and 2.4

Since Theorem 2.2 is a special case of Theorem 2.4 it suffices to prove the latter.

Let k be a positive integer, λ a partition of k, $q = p^\nu$ a prime power, $2 \leq m < k$, $D \in \mathbb{F}_q[t]$ monic with $\deg D = k - m - 1$ and $f \in \mathbb{F}_q[t]$. We are interested in the number of primes in the arithmetic progression $g \equiv f \mod D$, so we may replace f by $f - QD$, for some polynomial Q to assume that $\deg f < \deg D$. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$.

Let

$$\mathcal{F} = f + D\left(t^{m+1} + \sum_{i=0}^{m} A_i t^i\right) = \tilde{f} + D\left(\sum_{i=0}^{m} A_i t^i\right), \quad \tilde{f} = f + D \cdot t^{m+1},$$

where $\mathbf{A} = (A_0, \ldots, A_m)$ is an $(m+1)$-tuple of variables. Since $\deg \tilde{f} = m + 1 + \deg D = k > \deg D + m$, Proposition 3.6 gives that

$$\mathrm{Gal}(\mathcal{F}, \mathbb{F}(\mathbf{A})) = S_k,$$

Since $\deg \mathcal{F} = \deg_t \mathcal{F} = k$, Proposition 3.1 implies that the number N of $(a_0, \ldots, a_m) \in \mathbb{F}_q^{m+1}$ such that $f + D(t^{m+1} + \sum_{i=0}^{m} a_i t^i)$ has factorization type λ satisfies

$$\left|N - P(\lambda) q^{m+1}\right| \leq c_1(k) q^{m+1/2},$$

where $c(k) > 0$ is a constant depending only on k (and not on f, q).

Finally $\phi(D) = |D| \prod_{P|f} (1 - 1/|P|)$, where the products runs over the distinct prime polynomials P dividing D and since $|P| \geq q$, we have

$$\phi(D) = q^{\deg D}(1 + O(\frac{1}{q})) = q^{k-m-1} + O_k(q^{k-m-2}).$$

By Theorem 2.2 applied to the interval $I(t^k, k-1)$,

$$\pi_q(k; \lambda) = P(\lambda) q^k + O_k(q^{m+1/2}).$$

Thus

$$\left|\frac{\pi_q(k; \lambda)}{\phi(D)} - P(\lambda) q^{m+1}\right| \leq c_2(k) q^{m+1/2}$$

and

$$\left|N - \frac{\pi_q(k;\lambda)}{\phi(D)}\right| \le \left|N - P(\lambda)q^{m+1}\right| + \left|\frac{\pi_q(k;\lambda)}{\phi(D)} - P(\lambda)q^{m+1}\right| \le c(k)q^{m+1/2},$$

where $c = c_1 + c_2$. This finishes the proof since by definition $N = \pi_q(k; D, f; \lambda)$. □

6. Small m

In this section we show (3) fails in the cases excluded by Theorem 2.1 expect possibly in the case $p = m = 2$ and $\deg f' \le 1$ (when we do not know whether the (3) holds or not).

6.1. $m = 0$

We denote Euler's totient function by $\phi(k) = |(\mathbb{Z}/k\mathbb{Z})^*|$.

Proposition 6.1. *For $k > 1$ we have*

$$\pi_q(I(t^k, 0)) = \begin{cases} 0, & q \not\equiv 1 \mod k \\ \frac{\phi(k)}{k}(q-1), & q \equiv 1 \mod k. \end{cases}$$

In particular, if $k > 2$, $|\pi_q(I(t^k, 0)) - q/k| \gg q$.

Proof. We separate the proof into cases.

Case I. $\gcd(q, k) > 1$.

In this case $t^k - a$ is inseparable for any $a \in \mathbb{F}_p$. Since $\mathbb{F}_q$ is perfect, this implies that $t^k - a$ is reducible. So $\pi_q(I(t^k, 0)) = 0$.

Case II. $\gcd(q(q-1), k) = 1$.

In this case $k \neq 2$ and $1 - q$ is invertible modulo k. Assume, by contradiction, that there exists $a \in \mathbb{F}_q$ such that $f = t^k - a$ is irreducible in $\mathbb{F}_p[X]$. Then the Frobenius map, $\varphi\colon x \mapsto x^q$, acts transitively on the roots of f. Thus $\alpha^q = \zeta\alpha$, where ζ is a primitive k-th root of unity. We get that the orbit of α under φ is

$$\alpha \mapsto \alpha^q = \zeta\alpha \mapsto (\zeta\alpha)^q = \zeta^{1+q}\alpha \mapsto \cdots \mapsto \zeta^{1+q+\cdots+q^{k-1}}\alpha = \alpha.$$

On the other hand, this orbit equals to the set of roots of f which is $\{\zeta^i\alpha \mid i = 0, \ldots, k-1\}$. So for every $i \mod k$ there is a unique $1 \le r \le k$ such that

$$i \equiv 1 + q + \cdots + q^{r-1} \equiv (1-q)^{-1}(1-q^r) \pmod{k}.$$

This is a contradiction since there are at most $\phi(k) < k$ powers of $q \bmod k$, hence $\#\{(1-q)^{-1}(1-q^r) \mod k\} < k = \#\{i \mod k\}$.

Case III. $\gcd(q, k) = 1$ *and* $q \not\equiv 1 \mod k$.

Let $g = \gcd(q-1, k)$; then $l = k/g > 1$ and $\gcd(q(q-1), l) = 1$. Let $a \in \mathbb{F}_q$, and let α be a root of $f = t^k - a$. Then the polynomial $f_1 = t^l - \alpha^l \in \mathbb{F}_q[\alpha^l][t]$ is reducible by Case II. Since α is a root of g and since α^l is a root of $f_2 = t^g - a$, we get that

$$[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = [\mathbb{F}_q[\alpha] : \mathbb{F}_q[\alpha^l]] \cdot [\mathbb{F}_q[\alpha^l] : \mathbb{F}_q] < l \cdot g = k.$$

In particular f is reducible.

Case IV. $q \equiv 1 \mod k$.

In this case $\mathbb{F}_q$ contains a primitive k-th root of unity. By Kummer theory $t^k - a$ is irreducible in $\mathbb{F}_q$ if and only if the order of $a(\mathbb{F}_q^*)^k$ in $C = \mathbb{F}_q^*/(\mathbb{F}_q^*)^k$ is k. Since $\mathbb{F}_q^*$ is cyclic of order $q-1$, also C is cyclic of order k, hence there are exactly $\phi(k)$ cosets of order k in C. Each coset contains $\frac{q-1}{k}$ elements. So there are exactly $\frac{\phi(k)}{k}(q-1)$ irreducible $t^k - a$. □

6.2. $m = 1$ and $p \mid k$

In this case we study the interval $I(t^{p^2}, 1) = \{t^{p^2} - at + b \mid a, b \in \mathbb{F}_q\}$ for $q = p^{2n}$.

Proposition 6.2. *For $q = p^{2n}$ we have*

$$\pi_q(I(t^{p^2}, 1)) = 0.$$

In particular, $|\pi_q(I(t^p, 1)) - q^2/p| \gg q$.

Proof. Let $F = \mathbb{F}_{p^2}$, let E be the splitting field of $\mathcal{F} = t^p - At + B$ over $K = \mathbb{F}_q(A, B)$. Then, by [15, Theorem 2],

$$G = \mathrm{Gal}(\mathcal{F}, F) \cong \mathrm{Gal}(E/F) \cong \mathrm{Gal}(E \cdot \mathbb{F}, \mathbb{F}(A, B)) \cong \mathrm{Aff}(F),$$

as permutation groups. Here $\mathbb{F}$ is an algebraic closure of $\mathbb{F}_q$ and $\mathrm{Aff}(F)$ is the group of transformation of the affine line $\mathbb{A}^1(F) = F$:

$$M_{c,d} \colon x \mapsto cx + d, \quad 0 \neq c, d \in F.$$

Since $|G| = p^2(p^2 - 1)$ and since the group of translation $T = \{x \mapsto x + d\} \cong \mathbb{F}_{p^2}$ is of order p^2, we get that T is a p-sylow subgroup of T. But T is of exponent p, hence there are no p^2-cycles in G.

For every $a, b \in \mathbb{F}_q$, the Galois group $G_{a,b}$ of $f = t^{p^2} - at + b$ is a cyclic sub-quotient of G, hence of order $\leq p$. In particular $G_{a,b}$ acts intransitively on the roots of f, hence f is reducible. □

6.3. $m = 1$ and $p \mid k - 1$

The details of this case are nearly identical to Section 6.2 with the distinction that the group $\mathrm{Aff}(F)$ is replaced by the group of transformations on the projective line, cf. [15, Theorem 2]. Hence we state the result but omit the details.

Proposition 6.3. *For $q = p^{2n}$ we have*

$$\pi_q(I(t^{p^2}, 1) = 0.$$

A. Primes in almost all intervals

A.1. Generalities

Definition 1. Let Q be an infinite set of positive integers, and assume that for all $q \in Q$ we have a sequence $\mathcal{S}(q) = \{a_1(q), \dots, a_{n(q)}(q)\}$ of non-negative real numbers. We say that $\mathcal{S}(q)$

1. **converges on average to** 0 if $\frac{1}{n(q)} \sum_{i=1}^{n(q)} a_i(q) \to 0$ as $q \to \infty$.
2. **converges pointwise to** 0 if for any choice of a sequence of indices $i(q) \in [1, n(q)]$ we have $\lim_{q\to\infty} a_{i(q)}(q) \to 0$.
3. **converges almost everywhere to** 0 if for every $q \in Q$ there is a subset $J(q) \subseteq \mathcal{S}(q)$ such that $\lim_{q\to\infty} \#J(q)/n(q) = 1$ and for any choice of indices $i(q) \in J(q)$ we have $\lim_{q\to\infty} a_{i(q)}(q) \to 0$.

It is standard that convergence on average implies convergence almost everywhere:

Lemma A.1. *In the notation of Definition 1, if $\mathcal{S}(q)$ converges on average to 0, then $\mathcal{S}(q)$ converges almost everywhere to 0.*

Proof. Let $\epsilon > 0$. Since $\lim_{q\to\infty} \frac{1}{n(q)} \sum_{i=1}^{n(q)} a_i(q) = 0$ there exists $N_0(\epsilon) > 0$ such that for any $q > N_0(\epsilon)$ we have

$$\frac{1}{n(q)} \sum_{i=1}^{n(q)} a_i(q) < \epsilon^2. \tag{15}$$

Denote by

$$J(q) = \{1 \le i \le n(q) \mid a_i(q) < \epsilon\}.$$

Then, by (15), we have

$$\epsilon^2 > \frac{1}{n(q)} \sum_{i=1}^{n(q)} a_i(q) \ge \frac{1}{n(q)} \sum_{i \in [1,n(q)] \setminus J(q)} a_i(q) \ge \frac{n(q) - \#J(q)}{n(q)} \cdot \epsilon.$$

Thus $|1 - \#J(q)/n(q)| < \epsilon$, so $\lim_{q\to\infty} \#J(q)/n(q) = 1$.

Let $i(q) \in J(q)$. If $q > N_0(\epsilon)$, then $0 \le a_i(q) < \epsilon$, by the definition of $J(q)$, and hence $\lim_{q\to\infty} a_{i(q)}(q) = 0$. □

A.2. Number of primes in short intervals

In the terminology of Definition 1 Theorem 2.1 says that

$$\mathcal{E}(q) = \left\{ \left| \frac{\pi_q(I(f,m))}{q^{m+1}/k} - 1 \right| \;\middle|\; f \in M(k,q) \right\}.$$

converges pointwise to 0 (under the restrictions there on m). In what follows we show how to derive an almost everywhere convergence, including small m, from a result of Keating and Rudnick [9].

Definition 2. Let $f \in \mathbb{F}_q[t]$. The von-Mangoldt function, $\Lambda(f)$, is defined by

$$\Lambda(f) = \begin{cases} \deg(P) & \text{if } f = cP^k, \text{ where } P \text{ is a prime polynomial } P \text{ and } c \in \mathbb{F}_q^*, \\ 0 & \text{otherwise.} \end{cases}$$

If $f \in M(k,q)$ and $1 \le m < k$, we let

$$\nu(f;m) = \sum_{\substack{g \in I(f,m) \\ g(0) \neq 0}} \Lambda(g).$$

We denote the mean value and variance of $\nu(\bullet;m)$ by

$$\begin{aligned} \langle \nu(\bullet;m) \rangle &= \frac{1}{q^k} \sum_{f \in \mathcal{M}(k,q)} \nu(f;m), \\ \operatorname{Var} \nu(\bullet;m) &= \frac{1}{q^k} \sum_{f \in \mathcal{M}(k,q)} \left| \nu(f;m) - \langle \nu(\bullet;m) \rangle \right|^2, \end{aligned}$$

respectively.

Theorem A.2 (Keating-Rudnick)**.** *Let $1 \le m < k$ be integers. Then*

$$\langle \nu(\bullet;m) \rangle = q^{m+1} \left(1 - \frac{1}{q^k} \right). \tag{16}$$

If in addition $m < k-3$, then

$$\lim_{q \to \infty} \frac{1}{q^{m+1}} \operatorname{Var} \nu(\bullet;m) = k - m - 2. \tag{17}$$

Proof. See [9, Lemma 4.3] for (16) and Theorem 2.1 in *loc.cit.* for (17). □

Corollary A.3. *Let $1 \le m < k-3$ and for each prime power q let*

$$\mathcal{V}(q) = \left\{ a_f(q) = \left| \frac{\nu(f,m)}{q^{m+1}} - \left(1 - \frac{1}{q^k} \right) \right|^2 \;\middle|\; f \in \mathcal{M}(k,q) \right\}.$$

Then $\mathcal{V}(q)$ converges almost everywhere to 0.

Proof. By Theorem A.2 we have

$$\frac{1}{q^k}\sum_{f\in M(k,q)} a_f(q) = \frac{1}{q^k}\sum_{f\in M(k,q)}\left|\frac{\nu(f,m)}{q^{m+1}} - \left(1-\frac{1}{q^k}\right)\right|^2 = \frac{1}{q^{m+1}}\left(\frac{1}{q^{m+1}}\operatorname{Var}\nu(\bullet;m)\right)\to 0,$$

as $q\to\infty$. So $\mathcal{V}(q)$ converges to 0 on average. By Lemma A.1, $\mathcal{V}(q)$ converges almost everywhere to 0. □

The last corollary says that $\nu(\bullet;m)\sim q^{m+1}$ (as long as $1\le m<k-3$) almost always. It remains to explain how to deduce from this a similar result for the prime counting function.

For a short interval $I=I(f,m)$ with $f\in M(k,q)$ and for $d\mid k$ we let

$$I^{1/d} = \{g\in M(k/d,q)\mid g^d\in I\}.$$

Lemma A.4. *Let $f\in M(k,q)$, $1\le m<k$, $I=I(f,m)$ and $d\mid k$, $d>1$. Then*

$$\#(I^{1/d})\le q^m.$$

Proof. Let $J=I^{1/d}$. If $J=\emptyset$, we are done. Otherwise there is monic $g\in M(k/d,q)$ such that $g^d\in I$. Then $I=I(g^d,m)$, so without loss of generality we may assume that $g^d=f$.

If $\tilde g\in J$, then $\deg(\tilde g^d-f)\le m$. Moreover $\tilde g$ is monic, so $\tilde g=g+h$ for some h with $\deg h<k/d=\deg g$. It suffice to show that $\deg h<m$, since there are only q^m such polynomials.

If $d=p^a$, where $p=\operatorname{char}(\mathbb{F}_q)$, then $I\ni\tilde g^d=g^d+h^d=f+h^d$. So $\deg h\le m/d<m$ and we are done.

Assume $d=p^aD$ with $D>1$ and $\gcd(p,D)=1$. Write $g_1=g^{p^a}$ and $h_1=h^{p^a}$. Then $\deg h_1<\deg g_1$, $g_1^D=f$, and

$$\begin{aligned}\tilde g^d-f &= (g+h)^d-f=(g_1+h_1)^D-f\\ &= g_1^D+\textstyle\sum_{i=1}^D\binom{D}{i}g_1^{D-i}h_1^i-f = Dg_1^{D-1}h_1+\frac{D(D-1)}{2}g_1^{D-2}h_1^2+\cdots.\end{aligned}$$

Since $p\nmid D$ and $\deg h_1<\deg g_1$, we get that

$$m\ge\deg(\tilde g^d-f)=\deg(g_1^{D-1}h_1)=\frac{k(D-1)}{D}+\deg h_1>\deg h_1,$$

as needed. □

Finally we prove (3) almost everywhere.

Corollary A.5. *Let $1\le m<k-3$ be integers and for each prime power q let*

$$\mathcal{E}(q)=\left\{\left|\frac{\pi_q(I(f,m))}{q^{m+1}/k}-1\right|\;\middle|\; f\in M(k,q)\right\}.$$

Then $\mathcal{E}(q)$ converges almost everywhere to 0.

Proof. For $f \in M(k,q)$ and for $d \mid k$ we let $\Pi_d(f) \subseteq I(f,m)^{1/d}$ be the subset of monic prime polynomials of degree d and let $\epsilon = 1$ if $t^k \in I(f,m)$ and $\epsilon = 0$ otherwise. Then

$$\begin{aligned}\nu(f;m) &= \sum_{\substack{g \in I(f,m) \\ g(0)\neq 0}} \Lambda(g) = \sum_{g \in I(f,m)} \Lambda(g) + \epsilon = \sum_{d|k} \sum_{P \in \Pi_d(f)} d + \epsilon \\ &= k\pi_q(I(f,m)) + \sum_{\substack{d|k \\ 1<d\leq k}} \frac{k}{d} \pi_q(I(f,m)^{1/d}) + \epsilon.\end{aligned}$$

By Lemma A.4 we have $\pi_q(I(f,m)^{1/d}) \leq \#(I(f,m)^{1/d}) \leq q^m$ for $d > 1$. So

$$\nu(f;m) = k\pi_q(f,m) + O(c(k)q^m),$$

where $c(k) = \sigma(k) - k = \displaystyle\sum_{\substack{d|k \\ 1<d\leq k}} \frac{k}{d}$. Thus

$$\left|\frac{\pi_q(I(f,m))}{q^{m+1}/k} - 1\right| = \left|\frac{\nu(f;m)}{q^{m+1}} - 1\right| + O_k(q^{-1}) = \left|\frac{\nu(f;m)}{q^{m+1}} - \left(1 - \frac{1}{q^k}\right)\right| + O_k(q^{-1}).$$

Thus Corollary A.3 gives the convergence of $\mathcal{E}(q)$ to almost everywhere 0. □

Acknowledgments

We thank Zeev Rudnick for helpful remarks on earlier drafts of this paper and for the suggestions to consider arithmetic progressions and different factorization types.

The first two authors were supported by a Grant from the GIF, the German-Israeli Foundation for Scientific Research and Development. The last author was supported by the Göran Gustafsson Foundation (KVA).

References

[1] L. Bary-Soroker. Dirichlet's theorem for polynomial rings. *Proc. Amer. Math. Soc.*, **137**(1):73–83, 2009.

[2] L. Bary-Soroker. Irreducible values of polynomials. *Adv. Math.*, **229**(2): 854–874, 2012.

[3] S. D. Cohen. The Galois group of a polynomial with two indeterminate coefficients. *Pacific J. Math.*, **90**(1):63–76, 1980.

[4] A. Granville. Unexpected irregularities in the distribution of prime numbers. Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994), 388–399, Birkhäuser, Basel, 1995.

[5] A. Granville. Different approaches to the distribution of primes. *Milan J. Math.*, **78**(1):65–84, 2010.

[6] D. R. Heath-Brown. The number of primes in a short interval. *J. Reine Angew. Math.*, **389**:22–63, 1988.

[7] D. R. Heath-Brown and D. A. Goldston. A note on the differences between consecutive primes. *Math. Ann.*, **266**(3):317–320.

[8] M. N. Huxley. On the difference between consecutive primes. *Invent. Math.*, **15**:164–170, 1972.

[9] J. P. Keating and Z. Rudnick. The variance of the number of prime polynomials in short intervals and in residue classes. *Int. Math. Res. Not. IMRN*, page 30 pp., April 2012.

[10] S. Lang and A. Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, **76**:819–827, 1954.

[11] H. L. Montgomery and R. C. Vaughan. *Multiplicative Number Theory I. Classical Theory*. Cambridge Studies in Advanced Mathematics, 97. Cambridge University Press, Cambridge, 2007. xviii+552 pp..

[12] R. A. Rankin. The Difference between Consecutive Prime Numbers. *J. London Math. Soc.*, **13**:242–247, 1938.

[13] A. Selberg. On the normal density of primes in small intervals, and the difference between consecutive primes. *Arch. Math. Naturvid.*, **47**(6):87–105, 1943.

[14] J.-P. Serre. *Topics in Galois Theory (Research Notes in Mathematics) [Hardcover]*. A. K. Peters, Ltd., 2 edition, 2008.

[15] K. Uchida. Galois group of an equation $X^n - aX + b = 0$. *Tohoku Math. J. (2)*, **22**(4):670–678, 1970.